CLAIMS

What is claimed is:

1. An integrated circuit arrangement comprising: an integrated circuit device 100 having a plurality of magnetically-responsive circuit nodes 130-134; and a package 106 adapted to inhibit access to the integrated circuit device 100 and including a plurality of magnetized particles 120-125 therein, the magnetically-responsive circuit nodes 130-134 magnetically responding to the plurality of magnetized particles 120-125 such that a change in magnetic field collectively provided by the magnetized particles 120-125 renders a change in a magnetic state of at least one of the magnetically-responsive circuit nodes 130-134.

2. The integrated circuit arrangement of claim 1, further comprising: a detection circuit 160 adapted to detect the magnetic state of the magnetically-responsive circuit nodes 130-134 and, in response to a change in the magnetic state, to detect that the package 106 has been tampered with.

3. The integrated circuit arrangement of claim 2, wherein the detection circuit 160 includes a comparison circuit adapted to compare the detected magnetic state with a reference state and to detect tampering with the package in response to the detected magnetic state being different than the reference state.

4. The integrated circuit arrangement of claim 3, further comprising a memory adapted to store data representative of an untampered magnetic state of the magnetically-responsive circuit nodes, wherein the comparison circuit is adapted to compare the data stored in the memory with the detected magnetic state and to detect tampering with the package in response to the data stored in the memory indicating a different magnetic state than the detected magnetic state.

5. The integrated circuit arrangement of claim 4, wherein the memory includes a one-time programmable ROM.

6. The integrated circuit arrangement of claim 3, wherein the integrated circuit device is adapted to alter data stored in the integrated circuit in response to the comparison circuit detecting tampering with the package.

7. The integrated circuit arrangement of claim 3, wherein the integrated circuit device is adapted to set a tamper-detection flag in response to the comparison circuit detecting tampering.

8. The integrated circuit arrangement of claim 1, wherein the magnetically-responsive circuit nodes change in magnetic state in response to a sufficient amount of the package being removed to allow probing access to the integrated circuit device.

9. The integrated circuit arrangement of claim 1, wherein the magnetically-responsive circuit nodes change in magnetic state in response to a sufficient amount of the package being removed to expose a circuit element in the integrated circuit.

10. The integrated circuit arrangement of claim 1, wherein removal of a portion of the package sufficient to allow imaging access to the integrated circuit device renders the change in a magnetic state of the magnetically-responsive circuit nodes.

11. The integrated circuit arrangement of claim 1, wherein removal of a portion of the package sufficient to allow electrical access to the integrated circuit device renders the change in a magnetic state of the magnetically-responsive circuit nodes.

12. The integrated circuit arrangement of claim 1, wherein the package covers a substantial portion of the integrated circuit device, wherein the plurality of magnetized particles are distributed throughout the package and wherein removal of a portion of the package sufficient to allow access to the integrated circuit device renders the change in a magnetic state of the magnetically-responsive circuit nodes.

13. The integrated circuit arrangement of claim 1, wherein each magnetically-responsive circuit node includes a circuit element that resistively responds to a magnetic field generated by the magnetized particles.

14. The integrated circuit arrangement of claim 1, wherein each magnetically-responsive circuit node includes: a mini magnet susceptible to a change in magnetic state as a function of a magnetic field from the magnetized particles; and a circuit element that resistively responds to a magnetic state of the mini magnet, wherein the mini magnet of the at least one of the magnetically-responsive circuit nodes changes state in response to the change in magnetic field collectively provided by the magnetized particles.

15. An integrated circuit arrangement comprising: an integrated circuit chip; a plurality of magnetically-responsive memory elements adapted to store a logical state as a function of a magnetic state of a magnetic element applying a magnetic field to the magnetically-responsive memory element; a package covering at least a portion of the integrated circuit chip and preventing access to the portion of the integrated circuit chip; a plurality of magnetic particles in the package, at least some of the plurality of magnetically-responsive memory elements having a logic state that is responsive to a magnetic field

generated by at least one of the plurality of magnetic particles; and a tamper-protection circuit adapted to detect the logic state of the at least some of the plurality of magnetically-responsive memory elements and, in response to the detected logic state changing, detecting that the package has been tampered with.

16. An tamper-protection arrangement comprising: a package arranged to cover at least a portion of an integrated circuit chip having at least one magnetically-responsive element therein, the package being arranged to prevent access to at least a portion of the integrated circuit chip; a plurality of magnetic particles in the package and arranged to cause a detectable magnetic response in the at least one magnetically-responsive element; and a tamper-protection circuit adapted to detect the magnetic response of the at least one magnetically-responsive element.

17. The tamper-protection arrangement of claim 16, further comprising a tamper-response circuit adapted to alter a characteristic of the integrated circuit chip in response to the tamper-protection circuit detecting the magnetic response of the at least one magnetically-responsive element.

18. The tamper-protection arrangement of claim 17, wherein the tamper-response circuit is adapted to erase memory from the integrated circuit chip in response to the tamper-protection circuit detecting the magnetic response of the at least one magnetically-responsive element.

19. A method for protecting an integrated circuit device from tampering, the method comprising: detecting a magnetic state of a plurality of magnetically-responsive circuit elements in the integrated circuit device; and in response to detecting a change in the magnetic state of the plurality of magnetically-responsive circuit nodes, detecting that the integrated circuit device has been tampered with.

20. The method of claim 19, wherein detecting a magnetic state of a plurality of magnetically-responsive circuit nodes includes monitoring the magnetic state of the plurality of magnetically-responsive circuit nodes.